R5-26 SMS shall receive the following data from the user to identify the subscription version to be modified: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-27 SMS shall allow the following data to be modified in the subscription version:

Location Routing Number (LRN) - the identifier of the switches having portable NXXs and used by the service providers <- at least one LRN is required.

Due Date - date on which transfer of service from old facilities-based service provider to new service provider is planned to occur.

LIDB GTT data - network addressing information for routing to serving LIDB.

DPC type for LIDB features GTT - indicates whether Destination Point Code identifies the subsystem or a gateway STP.

CLASS GTT data - network addressing information for routing TCAP messages to the ported-to switch.

DPC type for CLASS features GTT - indicates whether Destination Point Code identifies the end office or a gateway STP.

R5-28 The following fields are for future use. The new facilities-based service provider may not be required to treat these fields as mandatory.

Billing Service Provider ID

End-User Location - Value

End User Location - Type

Future 1

Future 2

Future 3

R5-29 SMS shall revalidate the modified subscription version. This revalidation process shall include the validations defined in R5-18.

R5-30 If the version fails validation, SMS shall issue an appropriate error message to the request originator. The pending subscription version, which the user was attempting to modify, shall be retained with no changes.

R5-31 If the version passes validations, SMS shall mark the version with a status of pending in the SMS and shall issue an appropriate message to both old and new service providers indicating successful completion of the pending process.

R5-32 If for a version that passed validations, the Due Date has been modified SMS shall send a notifier to the old facilities-based service provider informing them of the new Due date.

5.1.2.2.2.2 Modification of an Active Subscription Version

R5-33 SMS shall receive data in support of modification of an active subscription version to change only specific data associated with an active subscription version.

R5-34 SMS shall invoke version creation functionality to create a new (pending) subscription version based on the active subscription version.

R5-35 SMS shall receive the following data from the user to identify the active subscription version is to be modified: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-36 SMS shall allow the following data to be modified in the newly created subscription version:

Location Routing Number (LRN) - the identifier of the switches having portable NXXs and used by the service providers <- at least one LRN is required.

LIDB GTT data - network addressing information for routing to serving LIDB.

DPC Type for LIDB features GTT - indicates whether Destination Point Code identifies the subsystem or a gateway.

GTT data for CLASS features - network addressing information for routing TCAP messages to the ported-to switch.

DPC type for CLASS features GTT - indicates whether Destination Point Code identifies the end office or a gateway STP.

R5-37 The following fields are for future use. The new facilities-based service provider may not be required to treat these fields as mandatory.

Billing Service Provider ID

End-User Location - Value

End-User Location - Type

Future 1

Future 2

Future 3

R5-38 SMS shall validate the modified subscription version. This validation process shall include the applicable validations defined in R5-18.

R5-39 If the version fails validation, SMS shall issue an appropriate error message to the request originator. A new subscription version shall not be created and no changes shall be made to the current active subscription version.

R5-40 If the version passes validation, SMS shall record the current date and time (i.e., system date and time) as the Activation Date and Time Stamp, shall mark the version with a status of sending in the SMS, and shall issue an appropriate message to the request originator indicating successful completion of the modify process.

R5-41 SMS shall activate the version in the network as defined in R5-51 through R5-61.

5.1.2.2.3 Conflict Subscription Version

An authorized NPAC user requests a subscription be placed in conflict or removed from conflict by associating an action of "conflict on" or "conflict off" with a version. This functionality is invoked when an authorized user requests that the version be placed in or removed from conflict.

5.1.2.2.3.1 Placing a Subscription Version in Conflict

R5-42 SMS shall receive the following data from the user to identify the subscription version is to be placed in conflict: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-43 If the version status is not pending, SMS shall generate an error message and send it to the request originator. SMS shall not proceed further with the request to place the subscription version in conflict.

R5-44 If the version status is pending, SMS shall mark the version with a status of conflict, shall record the current date and time (i.e., system date and time) as the **Conflict** Date and Time Stamp and shall issue an appropriate message to the request originator indicating successful completion of the process to place a subscription in conflict.

R5-45 If a subscription version remains in conflict for thirty days, SMS shall invoke cancellation processing as defined in R5-71 (tuneable parameter). The user ID for this transaction shall be the "SMS System ID."

5.1.2.2.3.2 Removing a Subscription Version from Conflict

R5-46 SMS shall receive the following data from the user to identify the subscription version is to be removed from conflict: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-47 If the version status is not in conflict, SMS shall generate an error message and send it to the request originator. SMS shall not proceed further with the request to remove the subscription version from conflict.

R5-48 If the version status is conflict, SMS shall validate the subscription version. This validation process shall include the applicable validations defined in R5-18.

R5-49 If the version fails validation, SMS shall issue an appropriate error message to the request originator. A new subscription version shall not be created and SMS shall not proceed further with the request to remove the subscription version from conflict.

R5-50 If the version passes validations, SMS shall mark the version with a status of pending in the SMS and shall issue an appropriate message to the request originator indicating successful completion of the process to remove a subscription from conflict.

5.1.2.2.4 Subscription Version Activation

A user requests a subscription be activated in the network by associating a network action of "activate" with a version. This functionality, which can be invoked only by the new facilities-based service provider enables an authorized user to request that a subscription version be activated.

R5-51 SMS shall receive the following data from the user to identify the subscription version is to be activated: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

SMS shall record the current date and time (i.e., system date and time) as the Activation Date and Time Stamp.

R5-52 If the version status is not pending, SMS shall generate an error message and send it to the request originator.

R5-53 SMS shall re-validate the subscription version as per the validations defined in R5-18.

R5-54 If the version fails re-validation, SMS shall log the error message(s) and make them available to authorized users, and mark the version status as invalid in the SMS.

R5-55 If the version is valid, SMS shall determine the Local SMS configuration data of all the Local SMSs.

R5-56 SMS shall translate the subscription version data to create interface messages containing the information to be updated to the Local SMSs.

R5-57 SMS shall send the interface messages to the Local SMSs. The subscription version shall be marked with a status of sending in the SMS. SMS shall record the current date and time (i.e., system date and time) as the Broadcast Date and Time Stamp in the subscription version.

R5-58 SMS shall log the activation responses resulting from the activation requests sent to the Local SMSs. SMS shall allow users (with the appropriate security permissions) to view this information. The length of time that data will remain in this log shall be a parameter that is tuneable by the SMS Administrator.

R5-59 If a positive acknowledgment is received from all involved Local SMSs, then the subscription version shall be marked with a status of active in the SMS and the previously active version (if one exists) for the same subscription (i.e., ported TN) shall be marked as old.

R5-60 If the version fails activation in some of the Local SMSs to which it was sent (e.g., the link between SMS and a specific network node is down), the update shall remain in queue and shall be resent to the Local SMSs where activation failed. The number of automatic resends and the interval between resends shall be parameters that can be modified by the SMS Administrator. There shall be a default of three (3) for the number of retries and a default of two (2) minutes for the interval between resends. During this period, the status of the version shall remain "sending." Once the maximum queue time is exceeded, SMS shall consider the version to have failed activation at specific Local SMSs. SMS shall mark the status of the previously active version (if one exists) for the subscription (i.e., ported TN) as old. SMS shall send a notification to the NPAC System Administrator. This notification shall include the list of the

Local SMS(s) where activation failed. Special processing must be invoked by the NPAC System Administrator to resend the subscription version to the Local SMS(s) where it failed activation. The subscription version shall be marked with a status of failed and an indication that the failure was partial.

R5-61 If the version fails activation in *all* the Local SMSs to which it was sent, SMS shall mark the status of the version as failed. If there is a current active subscription version, it shall remain active. SMS shall send a notification to the NPAC System Administrator indicating that the subscription failed activation at all Local SMSs. Special processing must be invoked by the NPAC System Administrator to resend the subscription. The subscription version shall be marked with a status of failed.

5.1.2.2.5 Disconnect Subscription Version

When a user requests that an active subscription be disconnected, it will be deleted from the network. This functionality, which can be invoked only by the new facilities-based service provider, enables the user to remove an active version from the network. The user-supplied Disconnect Date indicates when the customer's service was disconnected.

R5-62 SMS shall receive the following data from the user to identify the subscription version is to be deleted: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-63 If there is no subscription version with a status of active, SMS shall notify the request originator that the version is not active in the network and cannot be disconnected

R5-64 If there is a subscription version with a status of pending, invalid, failed, or conflict and there is also a subscription version with a status of active, SMS shall notify the request originator that the active version cannot be disconnected until the pending, invalid, failed, or conflict version is canceled. SMS shall not proceed with the request.

R5-65 If the status of the current version for the subscription is active, SMS shall do the following:

translate the pending disconnect request to create an interface message identifying the subscription to be deleted by the Local SMSs,

send the disconnect message to the Local SMSs, and

mark the disconnect request with the status sending. SMS shall record the current date and time (i.e., system date and time) as the Broadcast Date and Time Stamp in the disconnect request.

R5-66 If the disconnect request succeeds in all the Local SMSs, SMS shall mark the

current active subscription version with a status of old, shall update the Disconnect Date

to the old subscription version, and shall mark the disconnect request as old.

R5-67 If the disconnect request fails in all of the Local SMSs, the status of the disconnect request shall be changed to failed. The current active subscription version shall remain active. SMS shall send a notification to the NPAC System Administrator that the disconnect request failed. Special processing must be invoked by the NPAC System Administrator to resend the disconnect request to the Local SMS(s).

R5-68 If the disconnect request fails in some of the Local SMSs to which it was sent (e.g., the link between SMS and a specific network node is down), the disconnect request shall remain in queue and shall be resent to the Local SMSs where the disconnect failed. The number of automatic resends and the interval between resends shall be parameters that can be modified by the SMS Administrator. There shall be a default of three (3) for the number of retries and a default of two (2) minutes for the interval between resends. During this period, the status of the disconnect request shall remain "sending." Once the maximum queue time is exceeded, SMS shall consider the disconnect request to have failed at specific Local SMSs. SMS shall send a notification to the NPAC System Administrator. This notification shall include the list of the Local SMS(s) where the disconnect request failed. Special processing must be invoked by the NPAC System Administrator to resend the disconnect request to the Local SMS(s) where it failed. The disconnect request shall be marked with a status of failed and an indication that the failure was partial.

5.1.2.2.6 Subscription Version Cancellation

Only subscription versions with a status of pending, invalid, or conflict can be canceled. A user requests that a pending, invalid or conflict subscription be canceled in SMS by associating an action of "cancel" with a version. This functionality enables a user to cancel a subscription version that has not yet been activated in the network. Additionally, only NPAC personnel can cancel a subscription version with a status of conflict.

R5-69 SMS shall receive the following data from the user to identify the subscription version to be canceled:

the Local Number Portability Service ID and

the Ported Telephone Number Subscription ID.

R5-70 If there is no subscription version with a status of pending, invalid, or conflict, SMS shall issue an appropriate error to the request originator and shall not proceed with the request.

R5-71 If there is a subscription version with a status of pending, invalid, or conflict, SMS shall mark the subscription version with a status of canceled and record the current date and time (i.e., system date and time) as the **Cancellation** Date and Time Stamp.

5.1.3 Subscription Queries

The query functionality discussed in this section will give users the ability to view subscription data without being able to update that data. A user may not be able to modify a particular data item because that user does not have the proper security permissions and the data is made available via SMS for read-only purposes.

Assumptions

Users will need to be able to retrieve subscription data that they cannot modify.

Users shall submit query requests for subscription data based on a single ported TN only.

Any authorized service provider personnel shall be able to view any subscription version for any ported TN.

User Functionality

R5-72 An authorized SMS user shall be able to invoke the following functionality in the SMS to query subscription data:

Query data stewarded by SMS for a subscription and all its versions.

System Functionality

The following specifies SMS functionality needed to support the user requests defined above.

R5-73 For queries regarding subscription data, SMS shall receive the Local Number Portability Type ID and the Ported Telephone Number Subscription ID, and optionally, the status of the subscription version (e.g., active, pending).

R5-74 If multiple subscription versions are found, and the user has provided the status of the subscription version desired, SMS shall retrieve only the data associated with that status of the subscription version only. Otherwise SMS shall return all subscription version data associated with the ported TN. The parameters to be returned, as appropriate for the subscription version status, are as follows:

Local Number Portability Type ID

Ported Telephone Number(s)

Due Date

New facilities-based service provider ID

Old facilities-based service provider ID

Authorization from old facilities-based service provider

Authorization from new facilities-based service provider

Location Routing Number (LRN)

LIDB GTT data

DPC type for LIDB features GTT

CLASS GTT data

DPC type for CLASS features GTT

Billing Service Provider ID

End-User Location Value

End User Location Type

Future 1

Future 2

Future 3

Disconnect Date

Conflict Date and Time Stamp

Activation Date and Time Stamp

Broadcast Date and Time Stamp

Cancellation Date and Time Stamp

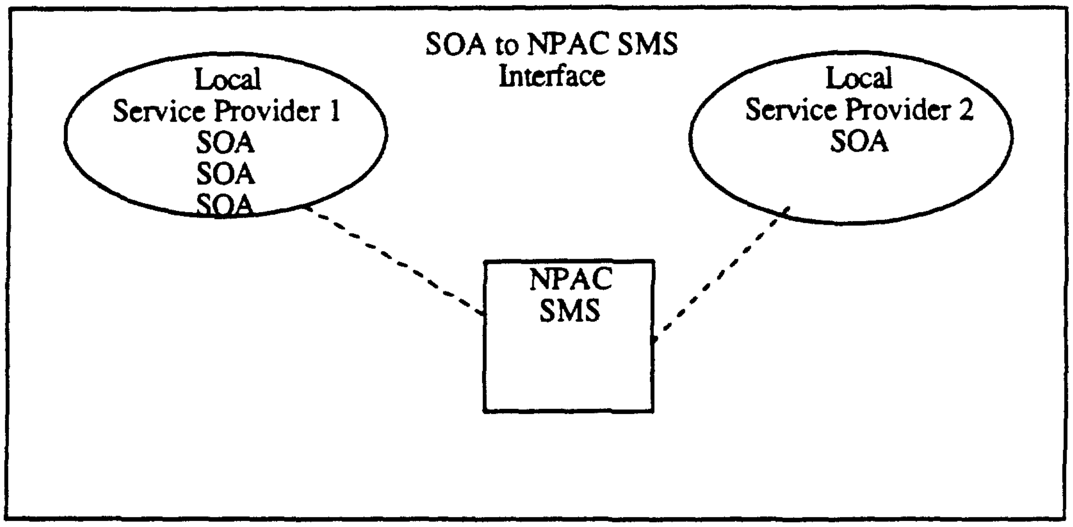
R5-74 If SMS does not have a subscription version as specified by the request originator, SMS shall provide the request originator with a message indicating that there was no data in SMS that matched the search keys.

Section 6: NPAC SMS Interfaces

Two interfaces to the NPAC SMS shall be supported. The first interface shall be between the NPAC SMS and the service provider's Service Order Activation platform and the second shall be between the NPAC SMS and the Local SMSs. Both of the interfaces shall support two-way communications.

6.1 SOA to NPAC SMS Interface

The SOA to NPAC SMS Interface could be used by a variety of local service provider systems for retrieving and updating subscription data in an NPAC SMS. The types of systems that are expected to use this interface are Service Provisioning OSs and/or Gateway Systems.



6.1.1 Request Administration

The SOA to NPAC Interface will support four types of transactions: subscription request and audit request transactions from the front end system (e.g., the SOA) interface users, and response and notification transactions from the NPAC SMS. The Interface will require security features to ensure that data is not corrupted by unauthorized access. Security management is outside the scope of the interface, however, the Interface user will be required to provide parameters to support security management at the NPAC SMS.

R6-1 Associations on these application to application interfaces must use strong authentication.

R6-2 Each subscription administration request sent over the Interface shall be capable of supporting multiple independent transactions. One failed item in a request will not cause other items in the request to fail. See ANSI standard T1.246, *Operations, Administration, Maintenance and Provisioning (OAM&P) - Information Model and Services for Interfaces between Operations Systems across Jurisdictional Boundaries to Support Configuration Management - Customer Account Record*

Exchange (CARE) for an example of a GDMO (ISO 10165-4) description of an interface that can deal with bunched transactions.

R6-3 Each subscription administration request shall be acknowledged with at least one response transaction from the NPAC SMS. Some requests may be acknowledged more than once. For example, after validation processing is completed a response transaction would be sent back to the user with either a positive acknowledgment or a negative acknowledgment with an error message indicating the results of the validation.

6.1.2 Subscription Administration

Subscription Administration provides functionality in creating or modifying subscriptions and activating or deleting them from the networks. Based on security parameters, users of the interface shall be able to do the following:

R6-4 Add new versions of subscription data, as well as cancel or modify a specific version of subscription data.

R6-5 Retrieve subscription data, including either specific versions of a subscription or all versions.

R6-6 Request the activation or deletion of subscription data.

6.1.3 Audit Requests

Audit Request functionality enables users to obtain audits of a specific subscription or group of subscriptions at all service provider networks or at select networks. Based on security parameters, users of the interface shall be able to do the following:

R6-7 Request that an audit be performed for a subscription or a group of subscriptions.

R6-8 Specify that an audit be performed at all service provider networks or at select networks.

R6-9 Each audit request sent over the Interface shall be capable of specifying a single subscription or a range of TNs and specific search parameters.

R6-10 Each audit request shall be acknowledged with at least one response transaction from the NPAC SMS. This response shall include an acknowledgment of whether discrepancies were reported by individual service providers and the identity of those providers. Audits which find no discrepancy shall receive one response. If discrepancies are found, there shall be one response per erred telephone number.

6.1.4 Notifications

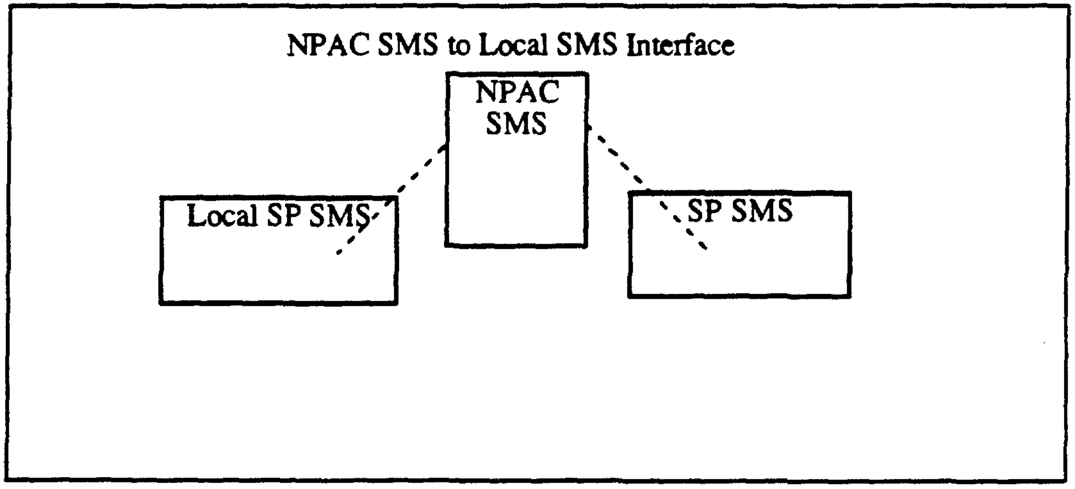
NPAC SMS shall have functionality to send notifications to service providers based on parameters which are tuneable by the NPAC SMS Administrator. NPAC SMS shall be able to do the following via the interface:

R6-11 Notify a new or an old service provider that they haven't provided authorization for a transfer of service for a TN.

R6-12 Notify an old service provider that the Due Date for a subscription has been modified.

6.2 NPAC SMS to Local SMS Interface

The NPAC SMS to Local SMS Interface could be used to send subscription data and audit requests to a variety of service provider systems. The types of systems that is expected to use this interface are Local SMSs (or SMS-like functionality at LNP SCPs) and/or Gateway Systems. The interface will require security features to ensure that data is not corrupted by unauthorized access. Security management is covered in Section 7, however, the interface user will be required to provide parameters to support security management at the NPAC SMS.



6.2.1 Transaction Administration

The NPAC SMS to Local SMS Interface will support five types of transactions: subscription download transactions from the NPAC SMS, audit requests from the NPAC SMS, network data download transactions from the NPAC SMS, response transactions from the Local SMS, and requests from the Local SMS that specific transactions be resent.

R6-13 Interface users shall specify their user-identification, system identification, and password to be able to use the Interface.

R6-14 Each subscription download request sent over the interface shall be capable of supporting multiple independent transactions. One failed item in a request will not cause other items in the request to fail.

R6-15 Each subscription download request shall be acknowledged with at least one response transaction from the Local SMS. A response transaction shall be sent back to the NPAC SMS with either a positive acknowledgment or a negative acknowledgment which may include a request that the transaction be sent again.

R6-16 Each audit request sent over the interface shall be for a single transaction or for a range of transactions.

R6-17 Each audit request shall be acknowledged with at least one response transaction from the Local SMS. A response transaction shall be sent back to the NPAC SMS with either a positive acknowledgment for those TNs which passed audit and a negative acknowledgment for those TNs which failed audit as well as only a negative acknowledgment for those TNs which failed audit.

R6-18 A local SMS shall be able to request the NPAC SMS to resend a subscription based on its TN or a block of subscriptions based on a time window specified in the request. This function might be provided by allowing for an audit request from the local SMS.

R6-19 Each network data download request shall be acknowledged with one response transaction from the Local SMS. A response transaction shall be sent back to the NPAC SMS with either a positive acknowledgment or a negative acknowledgment which may include a request that the transaction be sent again.

6.2.2 Network Subscription Administration

Network Subscription Administration provides functionality in activating, modifying, or deleting subscription data from the network and in requesting audits. The NPAC SMS, via its interface to Local SMSs shall be able to do the following:

R6-20 Add new subscription data, as well as delete or modify specific subscription data.

R6-21 Request audits of subscription data, including either a specific subscription or a range of subscriptions.

6.3 Interface Transactions

The CMIP protocol provides for seven types of transactions over the interface (Reference: ISO 9595 and 9596). They are Create, Delete, Set, Get, Cancel-Get, and Notification. The first six transactions are originated by the manager, and affect objects contained in the agent. The Notification transaction is created by the agent and is used to give notice to the manager that something of interest to the manager has happened to an object in the agent system.

R6-22 The object model shall be designed in terms of using these transactions in a manager-agent relationship.

6.4. Interface and Protocol Requirements

While it is expected that dedicated links will be used for the interfaces, switched connections should also be supported. Reliability and availability of the links will be essential and high capacity performance will be needed.

R6-23 The SOA to NPAC SMS Interface and the NPAC SMS to Local SMS Interface shall be an open, non-proprietary interface.

6.4.1 Protocol Requirements

Both of the NPAC SMS interfaces, as defined above, shall be implemented via the following protocol stack:

R6-24:

Application:	ASCE, CMISE/ROSE (ANSI T1.224)
Presentation:	as described in ANSI T1.224
Session:	as described in ANSI T1.224
Transport:	OSI Transport Class 0, RFC 1006, and TCP
Network:	Internet (IETF) IP
Link:	ethernet routing, or frame relay, or ATM (or more than one of these)
Physical:	as appropriate

R6-25 Multiple associations per service provider may be required.

6.4.2 Interface Performance Requirements

R6-26 Both the SOA to NPAC SMS and the NPAC SMS to Local SMS shall be available on a 24 by 7 basis.

R6-27 A 99.9 % availability rate shall be maintained for both interfaces.

R6-28 A transaction rate of 2 transactions per second shall be supported by each SOA to NPAC SMS interface association (See Section 10 for number of associations).

R6-29 A transaction rate of 25 transactions per second shall be supported by each NPAC SMS to Local SMS interface association (See Section 10 for number of associations).

6.4.3 Interface Performance Requirements

R6-30 The interoperable interface models shall be specified in terms of ISO 10165-4, "Generalized Definition of Managed Objects (GDMO)." The specification will become the property of the consortium, who may make it public.

R6-31 The model and interface specification shall be delivered in two stages.

R6-32 The model proposed shall be proposed shall be provided at the object and attribute level in the RFP proposal. It shall include tables and/or figures that show how the interface functions required by this specification were mapped into the services provided by the model.

R6-33 The selected Primary vendor shall deliver a complete interoperable interface specification one month after the announcement of the vendor selection.

R6-34 The application to application interfaces shall be specified in sufficient detail to allow the vendors who supply the SOA and Local SMS interfaces to build implementations that will interoperate with the NPAC SMS. This must be possible with no or only minimal interaction between the suppliers of the interoperable systems. For example the interoperable interface specification shall provide for error handling of error conditions appropriate to all of the functional requirements. It shall also define the security relationship between the systems.

R6-35 The interface specified shall be capable of extension to account for evolution of the interface requirements.

Section 7: Security Requirements

Intfoduction

In addition to the general security requirements based on the user interface paradigm in Section 7.1 through 7.7, there are requirements for the security on an OSI application to application interface (such as the one specified in Section 6 for the SMS to SMS and SMS to SOA interfaces). Section 7.8 describes such a security environment.

7.1 Identification

A user identification is a unique, auditable representation of the user's identity within the system. The SMS requires all system users, both individuals and remote machines, to be uniquely identified to support individual accountability.

R7-1 Unique user identification codes (userids) must be utilized to identify individuals and remote machines.

R7-2 SMS must require users, i.e., individuals and remote machines, to identify themselves with their assigned userid before performing any actions.

R7-3 SMS must maintain internally the identity of all currently active users.

R7-4 Every process running on SMS must have associated with it the userid of the invoking user (or the userid associated with the invoking process).

R7-5 SMS must disable userids after a period of time during which the userid has not been used. The time must be NPAC-specifiable with a system delivered default of 60 days.

R7-6 SMS must provide a complementary mechanism or procedure for the re-instatement or deletion of disabled userids.

R7-7 SMS must support the temporary disabling of userids.

R7-8 The mechanism that disables userids should provide an option for automatic reactivation.

R7-9 SMS must control and limit simultaneous active usage of the same userids by allowing only one active login. When the second login is entered, the system will ask if the first login can be disconnected. If the user replies yes, the second login can continue; however, if the user replies no, the second login is terminated.

7.2 Authentication

The identity of all system users, both individuals and remote machines, must be verified or authenticated to enter the system, and to access restricted data or transactions.

R7-10 SMS must authenticate the identity of all system users, both individuals and remote machines, prior to their initially gaining access to SMS.

R7-11 SMS must not support ways to bypass the identity authentication mechanisms.

R7-12 SMS must protect all internal storage of authentication data so that it cannot be accessed by any unauthorized user.

7.2.1 Password Requirements

R7-13 SMS shall not provide a mechanism whereby a single password entry can be shared by multiple userids.

R7-14 SMS must not prevent a user from choosing a password that is already associated with another userid.

R7-15 SMS must store passwords in a one-way encrypted form.

R7-16 Encrypted passwords must not be accessible to non-privileged users.

R7-17 Unencrypted passwords must not be accessible to any users, including NPAC personnel.

R7-18 SMS must automatically suppress or fully blot out the clear-text representation of the password on the data entry device, e.g., terminal.

R7-19 Passwords should not be sent over public or shared data networks in clear text.

R7-20 SMS must not allow for any password to be null.

R7-21 SMS must provide a mechanism to allow passwords to be user-changeable. This mechanism must require re-authentication of the user identity.

R7-22 The NPAC must have a mechanism to reset passwords.

R7-23 SMS must enforce password aging, i.e., passwords must be required to be changed after a NPAC-specifiable time. The system supplied default shall be 90 days.

R7-24 SMS must provide a mechanism to notify users in advance of requiring them to change their passwords. This can be done by one of the following methods:

(1) SMS will notify users a NPAC-specifiable period of time prior to their password expiring. The system supplied default shall be seven days.

(2) Upon password expiration, SMS will notify the user, but allow an NPAC-specifiable subsequent number of additional logons prior to requiring a new password. The system supplied default shall be two additional logins.

R7-25 Password must not be reusable by the same individual for an NPAC-specifiable period of time. The system supplied default shall be six months.

R7-26 SMS must provide a method of ensuring the complexity of user-entered passwords that meets the following requirements:

(1) Passwords must contain a combination of at least six alphanumeric characters including at least one alphabetic and one numeric or punctuation character. If the system does not distinguish between upper and lower case alphabetic characters, the minimum acceptable length is eight characters.

(2) Passwords must not contain the associated userid.

R7-27 SMS-supplied password generation algorithms must meet the following requirements:

(1) Passwords must be "reasonably" resistant to brute-force password guessing attacks, i.e., the total number of system generated passwords must be on the same order of magnitude as what a user could generate using the rules specified in requirement 7-26 (1) above.

(2) The generated sequence of passwords must have the property of randomness, i.e., consecutive instances must be uncorrelated and the sequences must not display periodicity.

7.3 Access Control

Access to the SMS and other resources must be limited to those users that have been authorized for that specific access right.

7.3.1 System Access

R7-28 SMS must allow access to authorized users and authorized remote systems.

R7-29 SMS must provide a procedure for the initial entry or modification of authorized users and authentication information.

R7-30 SMS must not provide any default userids that can permit unauthenticated SMS access.

R7-31 SMS's login procedure should be able to be reliably initiated by the user, i.e., a trusted communications path should exist between SMS and the user during the login procedure.

R7-32 SMS must disconnect or re-authenticate users after an NPAC-specifiable period of non-use. The system supplied default shall be 60 minutes.

R7-33 The SMS login procedure must exit and end the session if the user authentication procedure is incorrectly performed an NPAC-specifiable number of times. The system supplied default shall be three times.

R7-34 SMS must provide a mechanism to immediately notify the NPAC when the above threshold is exceeded.

R7-35 When the above threshold has been exceeded, an NPAC-specifiable interval of time, not to exceed 60 seconds, must elapse before the login process can be restarted on that I/O port.

R7-36 SMS must not suspend the userid upon exceeding the above threshold.

R7-37 SMS must perform the entire user authentication procedure even if the userid that was entered was not valid.

R7-38 Error feedback must provide no other information except "invalid," i.e., it must not reveal which part of the authentication information is incorrect.

R7-39 SMS should provide a mechanism to exclude or include users based on time-of-day, day-of-week, calendar date, etc.

R7-40 SMS should provide a mechanism to exclude or include users based on method or location of entry.

R7-41 SMS must provide a mechanism to limit the users authorized to access the system via dial-up facilities.

R7-42 SMS must provide a mechanism to limit system entry for privileged NPAC users on an NPAC-specifiable network access or per-port basis.

R7-43 Since some form of network access, e.g., dial-in, Wide Area Network, or Internet, is provided by SMS, SMS must provide a strong authentication mechanism. For example, the authentication mechanism could be a private or public key encryption-based mechanism, an additional password, and/or smart card to validate the user or remote system. For remote machines, public key encryption may be required in conjunction with dedicated private lines. For dial-in users (NPAC administrative and NPAC operations), smart cards are required.

R7-44 A mechanism must exist to end the session through secure logoff procedures. ,

R7-45 SMS must provide an advisory warning message upon system entry regarding unauthorized use, and the possible consequences of failure to meet those requirements.

R7-46 The message must be NPAC-specifiable to meet their own requirements, and any applicable laws.

R7-47 SMS must be able to display a message of up to 20 lines in length. This message should be displayed at the first point of entry. If possible, the message should appear before the logon process. As part of the delivered software, the following is an example of the default message that must be included:

NOTICE: This is a private computer system.

Unauthorized access or use may lead to prosecution.

R7-48 Upon successful access to the system, the following must be displayed:

(1) Date and time of the user's last successful system access.

(2) The number of unsuccessful attempts by that userid to access the system, since the last successful access by that userid.

R7-49 SMS must allow only the NPAC well-defined privileged users responsible for security administration to authorize or revoke users.

R7-50 Procedures for adding and deleting users must be well defined and described in the NPAC security documentation.

7.3.2 Resource Access

R7-51 Only authorized users shall be able to access the data that is part of or controlled by the SMS system.

R7-52 Each service provider's data must be protected from access by unauthorized users.

R7-53 Only authorized users shall be able to access the transactions, data, and software that constitute the SMS.

R7-54 The executable and loadable software must be access controlled for overwrite and update, as well as execution rights.

R7-55 Control of access to resources must be based on authenticated user identification.

R7-56 Encryption may be used to augment the access control mechanisms, but must not be used as a primary access control mechanism for sensitive data.

R7-57 For every resource controlled by SMS, it must be possible to grant access rights to a single user or a group of users.

R7-58 For every resource controlled by SMS, it must be possible to deny access rights to a single user or a group of users.

R7-59 It will be necessary to restrict user access to information based on the data content of a specific field, attribute, tuple, record, etc.

R7-60 Modification of the access rights to a resource must only be allowed by the NPAC.

R7-61 SMS must provide a mechanism to remove access rights to all resources for a user or a group of users.

R7-62 The access control mechanism's data files and tables must be protected from unauthorized access.

7.4 Data and System Integrity

R7-63 SMS must be able to identify the originator of any accessible system resources.

R7-64 SMS must be able to identify the originator of any information received across communication channels.

R7-65 SMS must provide mechanisms or procedures that can be used to periodically validate the correct operation of the system. These mechanisms or procedures should address:

(1) Monitoring of system resources
(2) Detection of error conditions that could propagate through the system
(3) Detection of communication errors above/below an NPAC-specifiable threshold
(4) Detection of Link Outages.

R7-66 SMS must be designed and developed to protect data integrity. This should include some or all of the following:

(1) Proper rule checking on data update
(2) Proper handling of duplicate/multiple inputs
(3) Checking of return status
(4) Checking of inputs for reasonable values
(5) Proper serialization of update transactions

R7-67 NPAC documentation must contain recommendations for running database integrity checking utilities on a regular basis.

7.5 Audit

7.5.1 Audit Log Generation

R7-68 SMS must generate an audit log that contains information sufficient for after-the-fact investigation of loss or impropriety and for appropriate response, including pursuit of legal remedies. The audit data shall be available on-line for a minimum of 90 days, and archived off-line for a minimum of two years.

R7-69 The user-identification associated with any SMS request or activity must be maintained, so that the initiating user can be traceable.

R7-70 SMS must protect the audit log from unauthorized access.

R7-71 Only well-defined privileged NPAC personnel can modify or delete any or all of the audit log.

R7-72 The audit control mechanisms must be protected from unauthorized access.

R7-73 SMS must cause a record to be written to the security audit log for at least each of the following events:

(1) Invalid user authentication attempts

(2) Logins and activities of NPAC users

(3) Unauthorized data or transaction access attempts

R7-74 Auditing of NPAC actions must not be able to be disabled.

R7-75 For each recorded event, the audit record must contain, at a minimum:

(1) Date and time of the event

(2) User identification including associated terminal, port, network address, or communication device

(3) Type of event

(4) Name of resources accessed

(5) Success or failure of the event

R7-76 Actual or attempted passwords must not be recorded in audit logs until after an NPAC-specifiable threshold of consecutive login failures. The SMS supplied default shall be three failures.

7.5.2 Reporting and Intrusion Detection

R7-77 SMS must provide post-collection audit analysis tools that can produce exception reports, summary reports, and detailed reports on specific data items, users, or communication failures.

R7-78 The NPAC must be able to independently and selectively review the actions of any one or more users, including other NPAC users, based on individual user identity.

R7-79 SMS must provide tools for the NPAC to monitor the activities of a specific network address or terminal in real time.

R7-80 SMS should contain a real-time mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent security violation. This mechanism shall be able to notify the NPAC immediately when thresholds are exceeded, and if the occurrence or accumulation of these security relevant events continues, SMS shall take the least disruptive action to terminate the event.

7.6 Continuity of Service

R7-81 No service provider action, either deliberate or accidental, should cause the system to be unavailable to other users.

R7-82 SMS should detect and report conditions that would degrade service below a pre-specified minimum.

R7-83 Procedures or mechanisms must be provided to allow recovery after a system failure or other discontinuity without a protection compromise.

R7-84 Procedures shall be documented for software and data backup and restoration.

R7-85 The system must contain a database containing the exact revision number of the latest software installed.

7.7 Software Vendor

R7-86 The SMS software vendor must have a corporate policy governing its internal development of software. This policy must contain specific guidelines and requirements that are aimed at the security of its products, and are applicable throughout the software life cycle.

R7-87 The SMS software vendor shall not design any mode of entry into the SMS for maintenance, support, or operations that would violate or bypass any security procedures.

R7-88 The SMS software vendor shall not design any mode of entry into the SMS for maintenance, support, or operations that is not a documented feature of the SMS.

7.8 OSI Security Environment

This section examines potential threats to the NPAC SMS interfaces and proposes a set of security requirements to thwart such threats.

The security mechanisms described in the OSI Security segment are meant to illustrate the level of security and flexibility that is required for the OSI interfaces specified. The response to the RFP may propose different security mechanisms than the ones described. However, such security mechanisms should provide at least the same level of security and at least the same level of flexibility as the mechanisms described. The proposed mechanisms shall not be more difficult to manage, and should not require more processing or transmission capacity than the mechanisms described below.

7.8.1 Threats

Attacks against the NPAC SMS may be perpetrated in order to achieve any of the following:

Denial of service to a customer by placing wrong translation information in the SMS

Denial of service to a customer by preventing a valid message from reaching the SMS

Disrupting a carrier's operations by having numerous spurious calls (to users who are not clients of that carrier) directed to that carrier

Switching customers to various carriers without their consent

Disrupting the functioning of the NPAC SMS by swamping it with spurious messages.

7.8.2 Security Services

The threats enumerated above can be thwarted by using the following security services:

R7-89 Authentication (at association setup)

R7-90 Data origin authentication for each incoming message

R7-91 Integrity - detection of replay, deletion or modification to a message

R7-92 Non-repudiation of origin

R7-93 Access control - allowing only authorized parties (i.e., carriers serving a given customer) to cause changes in the NPAC SMS database.

7.8.3 Security Mechanisms

This section outlines the requirements for specific security mechanisms to support the security services enumerated above. For simplicity of presentation and without loss of generality, it assumes that information in the NPAC SMS is modified only in response to CMIP notifications from authorized entities.

7.8.3.1 Encryption

R7-94 Since non-repudiation must be supported a Public Key Crypto System (PKCS) must be used to provide digital signatures. Since there is no requirement for confidentiality service there is no need for any additional encryption algorithms. The NPAC SMS shall support one of the digital signature algorithms listed in the OIW Stable Implementation Agreement, Part 12, 1995.

R7-95 If a digital signature based on RSA encryption is chosen then the size of the modulus of each key shall be at least 600 bits. If another algorithm is chosen then the size of the key(s) shall be chosen to provide a level of security commensurate with RSA encryption with a 600-bits modulus.

R7-96 The digital signature algorithm shall be applied to ASCII representation of the signed data fields, without any separators between those fields or any other additional characters.

7.8.3.2 Authentication

R7-97 Strong, two-way peer authentication at association setup time shall be provided by using an authenticator (based on the authenticator used for the Trouble Administration application of Electronic Bonding as described in Committee T1 Technical Report No. 40 "Security Requirements for Electronic Bonding Between Two TMNs") consisting of:

- The unique identity of the sender
- The Generalized Time corresponding to the issuance of the message, each party is responsible to assure that its system clock is accurate to within two minutes of GMT
- A sequence number (equal to zero for association request and association response messages)
- A key identifier
- Any additional parameters required by the chosen digital signature algorithm, as specified in OIW Stable Implementation Agreement, Part 12, 1995
- The digital signature of the sender's identity, GeneralizedTime and sequence number listed above.

R7-98 The authenticator shall be conveyed in the CMIP access control field. (An appropriate syntax for this EXTERNAL field shall be provided.)

7.8.3.3 Data Origin Authentication

R7-99 Every subsequent CMIP message that contains the access control field shall carry the authenticator described above in that field. Each party maintains a separate counter for the sequence number it uses. Every time the authenticator is used the value of the sequence number shall be incremented by one.

7.8.3.4 Integrity and Non-repudiation

R7-100 Because CMIP notifications do not have an access control field, all the notifications defined for the number portability application shall contain a security field. The syntax of the security field shall correspond to the authenticator defined above.

R7-101 The values of the components of the authenticator shall also be as specified for the authenticator above, except that the digital signature shall apply to all the fields in the notification, except the security field, in the order in which they appear, followed by the GeneralizedTime and the sequence number. This ensures data origin authentication, integrity and non-repudiation of origin for each notification. In particular, the GeneralizedTime and the sequence number allow detection of deletion, replay and delay.

R7-102 All the notifications shall be sent in the confirmed mode.

7.8.3.5 Access Control

R7-104 The NPAC SMS shall be responsible for access control. In particular, it will assure that only authorized parties (current and future service providers for a given customer) can change information related to the number associated with that customer.

R7-105 The only initiator-provided access control information that shall be used to this effect is the authenticated identity of the sender of the message that would result in a modification to the NPAC SMS database, and the value of the GeneralizedTime in that message (it should be within five minutes of the NPAC SMS system clock).

7.8.3.6 Audit Trail

R7-106 The NPAC SMS shall keep a log (as defined in ISO/IEC 10164 parts 6 and 8, 1992) of all incoming messages that result in the setup or termination of associations, all invalid messages (invalid signature, sequence number out of order, GeneralizedTime out of scope, sender not authorized for the implied request) as well as all incoming messages that may cause changes to the NPAC SMS database.

7.8.3.7 Key Exchange

R7-107 There shall be an exchange of keys between the NPAC and each carrier it serves. During this exchange each party shall provide the other with a list of keys. The list shall be provided in electronic form. The originator of list of keys shall also provide the receiver with signed (in ink) paper copy of the MD5 hashes of the keys in the list. The lists can be exchanged in person or remotely. If the lists are exchanged remotely, they shall be conveyed via at least two different channels (e.g., a diskette sent via certified mail and file sent via e-mail).

R7-108 Upon remote reception of a list of keys the recipient shall send an acknowledgment to the sender of the list. The acknowledgment shall consist of the MD5 hash of each one of the keys in the list. The acknowledgment shall be provided in electronic form via at least two different channels. In addition, the recipient shall call the sender by phone for further confirmation, and provide the sender with the MD5 hash of the whole list.

R7-109 The NPAC shall issue periodically (e.g., once a month) a paper list of the MD5 hashes of all the public keys it uses and those of its clients. The list shall be sent to each client. Upon reception of the list and verification of its own the NPAC's public keys hashes, the client shall return an acknowledgment (by phone or mail) to the NPAC.